Client Update – Part II
New SEC Cybersecurity Guidance: Focus on Governance

On February 21, 2018, the SEC issued new Guidance regarding cybersecurity disclosure and governance requirements applicable to SEC reporting companies. In our earlier Client Update on this topic, we discussed the disclosure considerations addressed in the Guidance. In this Client Update, we focus on the cyber-related governance issues addressed in the Guidance.[1]

CYBERSECURITY AND RISK GOVERNANCE

The Guidance addresses three governance topics in the context of cybersecurity: (1) the adoption and regular assessment of cyber-related disclosure controls and procedures; (2) the establishment of policies and procedures to address the risk of insider trading based on material nonpublic cybersecurity risks or incidents; and (3) compliance with Regulation FD when disclosing cybersecurity risks and incidents.

The SEC's focus on developing comprehensive policies and procedures related to cybersecurity and the need to guard against insider trading and selective disclosure is notable as those topics were not covered in the October 2011 guidance on cybersecurity issued by the Division of Corporation Finance.

Controls and Procedures

Building on the Sarbanes-Oxley Act and related SEC rules, the Guidance makes clear that appropriate and effective disclosure controls and procedures that enable companies to make accurate and timely disclosures of material events include "those related to cybersecurity." The Guidance notes that appropriate disclosure controls and procedures are essential to determine the potential materiality of cybersecurity risks and incidents to the company and its business, financial condition, and results of operations, and thus are crucial to a company's ability to make any required disclosure in the appropriate time frame. Specifically, companies should regularly assess whether their disclosure controls and procedures:

[1] The Guidance is available here.

- ensure that relevant information about cybersecurity risks and incidents is timely processed and reported to the appropriate personnel (*i.e.*, that they provide for open communications between technical experts and disclosure advisors, as well as up-the-ladder reporting to key decision makers);

- ensure timely collection and evaluation of information that is potentially subject to required disclosure or is relevant to an assessment of the need to disclose relevant developments and risks; and

- will appropriately record, process, summarize, and report the information related to the cybersecurity risks and incidents that are required to be disclosed in filings.

These types of controls and procedures should be generally consistent with disclosure controls and procedures that a public company already has in place with regard to the evaluation and disclosure of other material risks. However, it is worth noting that the nature of cyber-related matters and the intimate link with the technical side of the house may present new challenges when it comes to designing and implementing effective controls and procedures.

Sarbanes-Oxley CEO/CFO certifications regarding disclosure controls and procedures should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact. Similarly, the SEC expects a company's internal controls around financial reporting to be reasonably designed to capture the range and magnitude of the financial impacts of cyber incidents and ensure that those impacts are incorporated in the company's financial statements. The Guidance does not, however, explain how companies should assess the impact of a cyber incident on the effectiveness of its internal control over financial reporting.

Insider Trading

The Guidance encourages companies to consider how their policies, procedures, and controls account for and prevent trading on the basis of nonpublic information related to cybersecurity risks and incidents. Specifically, companies should review their insider trading policies and codes of ethics (as well as any related training) to assess whether they adequately guard against officers, directors, and other corporate insiders trading on the basis of (or otherwise misusing) material nonpublic information regarding cybersecurity incidents and risks.

Regulation FD

Given that information relating to cybersecurity incidents and risks may constitute material nonpublic information, companies may have disclosure obligations under Regulation FD in connection with nonpublic disclosures of those matters. Companies should review their policies and procedures relating to the selective disclosure of information (with a particular focus on their Regulation FD policies and related training). This review should assess whether these

policies and procedures are sufficient to prevent selective disclosures of material cybersecurity incidents and risks in violation of Regulation FD.

FINAL THOUGHTS

The Guidance does not introduce novel concepts and expectations. Instead, the Guidance emphasizes the need for companies to assess and, as appropriate, revise their policies, controls and procedures to ensure that they effectively address cyber-related matters.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Matthew E. Kaplan
mekaplan@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Paul M. Rodel
pmrodel@debevoise.com

Steven J. Slutzky
sjslutzky@debevoise.com

Joshua M. Samit
jmsamit@debevoise.com

Sandeep S. Dhaliwal
ssdhaliwal@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com